

【特許請求の範囲】

【請求項1】 ネットワーク端末をノードチャル間報道信ドメイン（VBDS）に接続するための方法であつて、
ネットワーク上においてネットワーク端末のユーパークを識別する情報を前記ネットワーク端末から受信する過程と、
1以上のVBDを含むユーパークを含む接続グループを決定する過程と、
前記ネットワーク端末が接続される以上のVBDを決定する過程であつて、前記
1以上のVBDが前記接続グループのメンバであるような前記決定過程と、
前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する
過程とを含むことを特徴とする方法。

【請求項2】 各VBDが、前記トライックが生じる前記VBDへの周報通信
トライックを制限可能なドメインのサブドメインであり、
前記接続グループが、少なくとも2つのドメインからVBDを含み、
前記ネットワーク端末が接続された以上のVBDが、前記ネットワーク端末を含
む前記ドメインに構成決定されることを特徴とする請求項1に記載の方法。

【請求項3】 各VBDがVLANであり、また前記ネットワーク端末が、前記
接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接
続されることを特徴とする請求項2に記載の方法。

【請求項4】 ネットワーク端末をノードチャル間報道信ドメイン（CVBDS）
に接続するための構造体であつて、
ネットワーク上においてネットワーク端末のユーパークを識別する情報を前記ネット
ワーク端末から受信する手段と、
1以上のVBDを含むユーパークの属する接続グループを決定する手段と、
前記ネットワーク端末が接続される以上のVBDを決定する手段であつて、前記
1以上のVBDが前記接続グループのメンバであるような前記決定手段と、
前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する
手段とを含むことを特徴とする構造体。

【請求項5】 各VBDが、前記トライックが生じる前記VBDへの周報通信
トライックを制限可能なドメインのサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、前記ネットワーク端末が接続されたID以上のVBDが、前記ネットワーク端末を含む前記ドメインに基づき決定されることを特徴とする請求項4に記載の構造体。

【請求項6】 各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項5に記載の構造体。

【請求項7】

(1) 前記構造体が、(1) 所定のコンピュータシステム、及び
(2) 前記コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々を含むことを特徴とする請求項4に記載の構造体。

【請求項8】

前記構造体が、所定のコンピュータの読み取り可能な媒体であり、そこで各手段が、以上のコンピュータの命令、コンピュータの読み取り可能なデータ、又は以上の命令及びデータの組合せを含むことを特徴とする請求項4に記載の構造体。

【請求項9】

1以上の装置に対して1以上のアクセス制御リスト (ACLs) を生成するための方法において、そのような装置にACLが与えられた場合に、前記ACLを用いて前記ドメイン間ににおいてどのようなトライックが許可及び／又は拒否されるかを決定し、更に、

サブネットワークの各グループ内においてトライックが許可されるように、サブネットワークのID以上のグループを規定する過程であって、各サブネットワークがネットワークドメインの一端であるか、或いはネットワークドメインの全てであり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、前記コンピュータシステムが、各グループ内のトライックを許可するためにID以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項10】

前記1以上のトライックが異なるグループにおけるサブネットワーク間のトライックを拒否する前記複数のグループを規定する過程を含むことを特徴とする請求項9に記載の方法。

【請求項1-1】 1以上の共同サブネットワークの識別子を受信する前記コンピュータシステムを更に含む前記方法において、トライフィックが、前記グループの何れか1つに於ける各共用ネットワークと任意の別のサブネットワークの間において許可され、

1以上のACLによって、トライフィックが、前記グループの何れか1つにおける前記共同サブネットワークとの間ににおいて許可されることを特徴とする請求項9に記載の方法。

【請求項1-2】 少なくとも1つの前記ドメインが、前記ドメインにおいて、前記トライフィックを制限することが可能であるような前記方法であつて、1以上のグループの各々に対して、前記コンピュータシステムが、前記グループ内において許可及び／又は拒否されたトライフィックを識別するための情報を受信する過程であつて、前記情報を、制限するトライフィックにおける1以上のドメインによって使用されるような前記受信過程と、前記情報による指定に従つてトライフィックを許可及び／又は拒否するように、前記コンピュータシステムがトライフィックを制限可能な各ドメインを構成する過程とを更に含むことを特徴とする請求項9に記載の方法。

【請求項1-3】 所定のグループ内において許可及び／又は拒否されたトライフィックを識別するための情報が、1以上の（1）トライフィックを制限可能なドメイン内のトライフィックを各々送信する以上のスイッチのポートであつて、前記グループ内のトライフィックを運ぶための前記ポートと、（2）前記グループに属するエンティティの物理的なアドレスと、更に（3）前記グループ内のトライフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項1-2に記載の方法。

【請求項1-4】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項9に記載の方法。

【請求項1-5】 前記1以上の装置が、IPアドレスに基づきトライフィックの経路を指定し、また各ドメイン内において、トライフィックが物理的なアドレスに基づき端末間で送信されることを特徴とする請求項9に記載の方法。

【請求項1-6】 ネットワークドメイン間のトライフィックの経路を指定す

る以上のお客様に対して以上的アクセス制御リスト（ACLs）を生成するための所定の構造体において、そのような状態にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間ににおいてどのようなトライックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトライックが許可されるよう、サブネットワークの以上とのグループをコンピュータシステムに対して規定する手段であつて、各サブネットワークがネットワークメインの一部であるか、或いはネットワークドメインの全であり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって讀取るための前記規定手段と

前記コンピュータシステムによって、各グループ内のトライックを許可するための以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項1-7】 前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項1-6に記載の構造体。

【請求項1-8】 前記構造体が、前記規定手段及び前記生成手段を実施するための命令を含むコンピュータの読み取り可能な媒体であることを特徴とする請求項1-6に記載の構造体。

【請求項1-9】 前記規定手段が複数のグループを規定するときには、前記1以上のACLが異なるグループにおけるサブネットワーク間のトライックを拒否することを特徴とする請求項1-6に記載の構造体。

【請求項2-0】 1以上の共用サブネットワークの識別子を前記コンピュータシステムによって読み取るための手段を更に含む前記構造体において、前記グループの何れか1つにおける各其用サブネットワークと他の任意のサブネットワークとの間でトライックが許可され、
1以上の前記ACLによつて、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任他のサブネットワークとの間でトライックが許可されることを特徴とする請求項1-6に記載の構造体。

【請求項2.1】 少なくとも1つの前記ドメインが、前記ドメインにおけるトライックを制限可能な、前記グルーブ内における記載構造体であって、以上のグルーブの各々に対して、前記グルーブ内における許可及び／又は拒否されたトライックを識別するための情報を前記コンピュータシステムによつて読み取るための手段であつて、前記情報が、トライックの制限において1以上のドメインによる指定を従つてトライックを許可及び／又は拒否するよう、前記情報による指定を従つてトライックを許可及び／又は拒否するように、トライックを制限可能な各ドメインを前記コンピュータシステムによつて構成するための手段とを更に含むことを特徴とする請求項1.6に記載の構造体。

【請求項2.2】 所定のグルーブ内において許可及び／又は拒否されたトライックを識別するための情報が、1以上の(1)トライックを制限可能なドメイン内のトライックを各々送信する以上のスイッチのポートであつて、前記グルーブ内のトライックを通ぶための前記1以上のポートと、(2)前記グルーブに属するエンティティの物理的なアドレスと、更に(3)前記グルーブ内のトライックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項2.1に記載の構造体。

【請求項2.3】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項1.6に記載の構造体。

【請求項2.4】 前記1以上の装置が、IPアドレスに基づきトライックの経路を指定し、また各ドメイン内において、トライックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項1.6に記載の構造体。

【請求項2.5】 複数のドメインを含む所定のネットワークにおける接続を確立するための方法において、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメインを有することができ、前記ドメインによつて、單一のサブドメイン内のトライックが許可されるが、サブドメイン間のトライックが拒否され、更に、各グルーブ内においてトライックが許可されるよう1以上の接続グルーブを規定する過程であつて、少なくとも1つの接続グルーブに対して、コンピュータシステムに前記接続グルーブに属するトライックを規定する情報を与えるよ

うな前記規定過程と、

少なくとも1つの接続グループに対し、前記コンピュータシステムに前記接続グループのメンバであるサブドメインの識別子を与える過程と、
少なくとも1つの接続グループに対して、前記サブドメインによって前記接続
グループにおけるトラフィックが許可されるよう、前記コンピュータシステム
が、前記接続グループにおけるサブドメインを構成する過程
とを含むことを特徴とする方法。

【請求項 2 6 1】 トライックを規定する前記情報が、少なくとも1つの
グループに対して、以下の(1) 単一のドメイン内のトライックを各々送信
する以上のスイッチのポートであって、前記グループ内のトライックを運ぶ
ための以上の前記ポートと、(2) 前記グループのメンバである端末の物理的
アドレスと、更に(3) 前記グループ内のトライックの送信又は受信を許可さ
れたユーザ名との識別子を含むことを特徴とする請求項 2 5 に記載の方法。

【請求項 2 7 1】 各々のドメインを構成する過程が、前記グループにおける
各サブドメインを有する単一のドメイン内のトライックを送信するスイッチに
ついて、(a) 前記グループのメンバである端末の物理的アドレス間のトライ
ックを許可するための、また(b) 異なるグループのメンバが許可されるが、サブドメイン間の
アドレス間のトライックを拒否するための前記スピッチャを構成する過程を含む
ことを特徴とする請求項 2 6 に記載の方法。

【請求項 2 8 1】 複数のドメインを含む所定のネットワークにおける接続
を確立するための構造体において、少なくとも1つのドメインが、前記ドメイン
において規定されたサブドメインを有することが可能であり、前記ドメインによ
つて、単一のサブドメイン内のトライックが許可されるが、サブドメイン間の
トライックが拒否され、更に、
以上の接続グループのセットに於ける各接続グループに属するトライック
を規定する情報をコンピュータシステムによって送信するための手段であって、
トライックが各グループ内で許可されるような前記送信手段と、

少なくとも1つの接続グループについて、前記接続グループのメンバであるサ
ブドメインの識別子を前記コンピュータシステムによって送信する手段と、

少なくとも1つの接続グループについて、前記サブドメインによって前記接続グループにおけるトラフィックが許可されるよう、前記接続グループにおいてサブドメインを有する各ドメインを前記コンピュータシステムによって構成するための手段とを含むことを特徴とする所定の構造体。

【請求項29】　トラフィックを規定する前記情報が、少なくとも1つのグループに対して、以上の(1)單一のドメイン内のトラフィックを各々透信する以上のスイッチのポートと、(2)前記グループ内のメンバである端末の物理的アドレスと、更に(3)前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項28に記載の構造体。

【請求項30】　前記構造体が、前記コンピュータシステム及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項28に記載の構造体。

【請求項31】　前記全ての手段を実施するための命令を含むコンピュータの読み取り可能媒体であることを特徴とする請求項28に記載の構造体。

【請求項32】　各ドメイン内のトラフィックが、端末の物理的アドレスに基づき端末間で送信され、またドメインのトラフィックが、端末の論理的アドレスに基づき経路指定されることを特徴とする請求項28に記載の構造体。

【発明の詳細な説明】

【0001】

発明の概要

本発明はネットワークに関するもので、また詳細にはネットワークにおいて接続性の確立に係るものである。

【0002】

セキュリティ上の理由やネットワークの通信量を低減する目的で、幾つかのネットワークでは接続を制限している。従って、ネットワークにおける幾つかの端末が互いに通信を許可される一方で、別の端末は通信を許可されない。接続性は、通信を許可された端末間の物理的な通信リンクが確立されることによって可能となるか、或いは通信を許可されていない端末間の物理的な通信リンクが確立されないことによって禁止され得る。しかし、これは各セットの接続の制限のための物理的リンクを個別に構成することが必要であるので実際的ではない。従って、コマンドを発行してネットワーク装置を割当することによってネットワークの接続性を確立する取扱いは変更するための技術が発達してきた。

【0003】

これについて図1及び図2に示す（これらの場合には先行技術にはない本発明の幾つかの特徴が示してある）。ネットワーク110には、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク110には、「第2層ドメイン(ayer 2 domains)」116P、116Q、116R、116S、116Tが含まれる（用語「第2層」は、D. Biererらの“NetWare^{3.4} for Professionals”（1993）、1-9頁（ここで省略することにより本明細書の一部とする）に記載のOSI参照モデルのを指す）。同一の第2層ドメイン116に属する端末124（例えは、ドメイン116Pにおける端末124-1、124-2）は、それらのMACアドレス（「第2層」アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインターフェースカード（NIC）に書き込まれた物理的アドレスであるか、又はNICスイッチの設定によって確立された物理的アドレスである。全てのドメイン116又はその幾つかには、以上のネットワークスイッチ（NICスイッチと混同しない）が含まれ得る。各ドメイン116のスイッチ128は

【0004】

異なる第2層ドメインにおける端末（例えば、端末124.1、124.3）は、MACアドレスのみを使用して互いに通信することはできない。それらは、論理アドレスであるIPアドレスを用いて通信する。ルータ130.1、130.2、130.3は、端末のIPアドレス（必要に応じてIPアドレスとMACアドレスとの間で変換される）に基づきドメイン1.1.6間のトライックの経路を指定する。

【0005】

幾つかのドメイン1.1.6においては、ハーチャルLAN（即ち、VLAN）を用いて接続性を制限することができます。例えば、ドメイン1.1.6Pには3つのVLAN 1.4.0a、1.4.0b、1.4.0cが含まれる（図2）。ドメイン1.1.6Pにおける端末1.2.4は、それらが同じ…のVLANに属している場合にのみ、第2層において（即ち、それらの第2層アドレスを用いて）互いに通信可能である。前述して、図1に示すVLAN 1.4.0aに属する端末124.1、124.2は通信可能である。

【0006】

VLANは、LANスイッチ1.2.8によって実現される。詳述すると、スイッチ1.2.8は、同一のVLAN内の端末間のみでパケットを送信する。（スイッチ1.2.8は、VLANへのトライックを制限可能なため、VLAN…capableと称される。例えば、ドメイン1.1.6S、1.1.6Tのような幾つかの第2層ドメインには、非VLAN…capableスイッチが含まれ得る。）

異なる第2層ドメイン間の接続は、ルータ1.3.0によって制限される。ルータ1.3.0は、IPアドレスに基づき接続の制限を規定するアクセス制御リスト（ACLs）を使用する（例えば、K. Sivyan及びC. Bareの”Internet Firewalls and Network Security”（1995）、187-192頁を参照）。

【0007】

アクセス制御リストの作成及びVLANの規定は、ネットワーク管理を混乱させること例なプロセスであり得る。このプロセスは、動的ネットワーク環境においては度々繰返されねばならず、そこでは端末、ユーザ、及びネットワークサービスが異なる場所から別の場所へ移動し、又は物理的な移動なしに既存の組織から他の組織へ

織へ移され、或いは付加もしくは除去される。
(11)

【00081】

従つて、ネットワークにおける接続の設定を容易にすることが望ましい。

【0009】

発明の問題

本発明は、ネットワークの接続を確立及び制御するための新しい方法とシステムを提供するものである。幾つかの実施例においては、VLAN及びアクセス制御リストの容易な生成が可能となる。

【0010】

幾つかの実施例においては、アクセス制御リストが管理端末(Management station)によって作成される。管理端末は接続グループの規定を保管する。各接続グループ(connectivity groups)はサブネットワークのグループである。トライフィックは各グループの中に許可される。幾つかの実施例において、各サブネットワークはIPサブネットとして識別される。管理端末は、接続グループを規定する情報からアクセス制御リストを作成する。

【0011】

幾つかの実施例において、管理端末は共用サブネットワークの識別子を受信し、また任意の接続グループにおける任意のサブネットワークと共用サブネットワークとの間のトライフィックを許可するACLを生成する。

【0012】

幾つかの実施例において、管理端末は、例えばVLANのようなサブドメインを、ドメインを適切に構成することによって生成する。ネットワーク管理者は、ドメインを構成するためにそのグループに属するトライフィックを規定する各接続グループ情報を入力する。そのような情報の例には、同一の接続グループに属するエンティティ(例えば、スイッチのポート、ネットワーク端末のMACアドレス、又はロダジョン時にユーザによって指定されるユーチャ名)のリストが含まれる。異なる接続グループからは、エンティティは、異なる第2層ドメインからのエンティティを含み得る。エンティティは、どのエンティティがどのVLANに属するかを指定することなしに、接続グループに対して割

当てられ得る。管理端末は、同一のグループにおける何れのエンティティが所定の組…のドメインに属するかを決定し、そのようなエンティティを適切なVLANに配置する。

【0013】

幾つかの実施例において、接続グループにおけるトラフィックを規定する情報には、第2層パケットのビットの箇数が含まれる。

【0014】

本発明は、第2層ドメイン、スイッチ、又はレータに限られるものではない。本発明の他の特徴及び優位性については後述する。本発明は添付した請求の範囲で規定されるものである。

【0015】

発明の詳細な説明

ネットワーク110には、5つの第2層ドメイン116が含まれる。各ドメインにおけるパケットのアドレス指定が、OSI参照モデルの第2層（データリンク層）におけるパケットの内容に基づいて行われるので、これらのドメインは「第2層」と称される。ルータ130は、第3層（ネットワーク層）におけるパケットの内容に基づきトラフィックの経路を指定する。特に、IPアドレスは、第3層のアドレスである。しかし、本発明は第3層又はOSI参照モデルに従うネットワークに限定されるものではない。

【0016】

ドメイン116内には、MACアドレスに基づきトラフィックを送信するVLAN-capableスイッチ128-1、128-2が含まれる。それらのスイッチは、トランク150-1によって互いに接続されている。各スイッチは、ネットワークセグメントに各々接続されている以上のポートを有する。従つて、スイッチ128-1のポート160-1は、端末124-1を含むネットワークセグメントに接続されている。また、スイッチ128-2のポート160-2は、端末124-2を含むネットワークセグメントに接続されている。図1において、各ネットワークセグメントは単一の端末を含む。或る実施例においては、ネットワークセグメントは複数の端末を含む。

【0017】

スイッチ128.1のポート160Mは、後述するような接続グレーブの生成に用いられる管理端末124Mに接続される。

【OO18】

スイッチ128.1は、トランク150.2によつてルータ130.1に接続される。ルータ130.1は、ルータ130.2、130.3、及びインターネット170に接続される。ルータ130.2は、ルータ130.3に接続される。ルータ130.2は、トランク150.3によつてドメイン116QのVLAN-capableスイッチ128.3に接続される。ドメイン116Qには、VLAN-capableスイッチ128.4、128.5、及び128.6が含まれ、その各々はスイッチ128.1、128.2と同様に1以上的ネットワークセグメントに接続される。ここでは、端末124.3を含むセグメントのみ示す。また、ドメイン116Qのスイッチ128は互いに接続している。

【OO19】

ルータ130.2は、第2層ドメイン116Tに接続されている。

【OO20】

ルータ130.3は、ドメイン116RのVLAN-capableスイッチ128.7及び第2層ドメイン116Sに接続されている。スイッチ128.7は、スイッチ128.1、128.2と同様にネットワークセグメント(図示せず)に接続されている。ドメイン116S、116Tはスイッチを全く含まないか、或いは幾つかのスイッチ(図示せず)を含む。

【OO21】

幾つかの実施例において、以上のドメイン116はスイッチを全く含まないか、或いは非VLAN-capableスイッチ、ハブ又はコンセントレータ含む。

【OO22】

前述のように、異なるドメイン間の通信にはIPアドレスが使用される。例えば、端末124.3がパケット1を送信するために、端末124.1は、端末124.3のIPアドレス及びルータ130.1のMACアドレスを、それで物理的ルート先アドレスとしてパケットに書き込み。ルータ130.1は、宛先MACアドレスをルータ130.1のMACアドレスと書き換え、端末124.1の発信元MACアドレスをルータ130.1のMACアドレスに書き換える。次にルータ130.1が、パケットをルータ130.2に送

信する。ルータ130,26は、パケットの発信元MACアドレスを自身のMACアドレスに書き換えて、また宛先MACアドレスを端末124,3のMACアドレスに書き換えて、パケットをスイッチ128,3に送信する。スイッチ128,3は、パケットをスイッチ128,5経由で端末124,3に送信する。ドメイン116Pには複数していないVLAN140a、140b、140c(図2)が含まれ、ドメイン116Qには、重複していないVLAN140d、140e、140fが含まれ、ドメイン116Rには重複していないVLAN140g、140h、140iが含まれる。VLANにおける端末のメンバーシップは、端末が接続されているスイッチポート160によって規定されるか、端末のMACアドレスによって規定されるか、或いは端末にログオンしたユーザのユーザ名によって規定される。ポート又はMACアドレスに基づくVLANのメンバーシップの確定については、G. Heldの“Virtual LANS: Construction, Implementation, and Management”(1997), 233-249頁(ここで著者により本明細書の一部とする)に開示されている。

【00231】

ユーザー名によるVLANのメンバーシップの確定については、付録Aに記載されている(“User-Based Binding of Network Stations to Broadcast Domains”と題する)。Ekstromらの米国特許H108/832,011(1997年4月2日出願;ここで著者により本明細書の一部とする)を参考)。或る実施例においては、VLAN140が、ポートによって識別される端末、MACアドレスによつて識別される端末、及び／又はユーザ名によつて識別される端末を結び付ける。

【00241】

ドメイン116S、116Tは、任意のVLANを含む場合もあり、また含まない場合もある。

【00251】

管理端末124Mは、VLAN140bに属する。端末124Mは、任意のスイッチ128及び任意のルータ130と通信可能である。或る実施例において、(1)全てのスイッチ128は、Cisco社(San Jose, California)から入手可能なType Catalyst[®]のスイッチであり、また(2)ルータ130は、Cisco社から入手可能なルータであり、それらはCisco社の説明書に記載されている(部品番号7

(15)

特表2 0 0 2-5 1 3 2 4 5

【0 0 2 6】

ネットワーク 1 1 0 には、種々のドメイン 1 1 6 におけるエンティティ (特にトランクスイッチポート 1 6 0、MACアドレス、又はユーナーが名) を含む接続グループが含まれる。例えば、接続グループは、VLAN 1 4 0 a、1 4 0 d、1 4 0 g における全てのエンティティによって構成され得る。通信は、同一の接続グループにおけるエンティティ間ににおいては許可され、異なる接続グループにおけるエンティティ間ににおいては拒否される。詳述すると、スイッチ 1 2 8 及びルータ 1 3 0 は、或る接続グループにおける端末 1 2 4 から別の接続グループにおける端末 1 2 4 へのペケットの経路は指定しない。

【0 0 2 7】

周知のように、VLAN は回報通信ドメインである（また、ここでは「第2層回報通信ドメイン」又は「第2層 BD」と称される）。対照的に、接続グループは必ずしも回報通信ドメインではない。従って、幾つかの実施例においては、回報通信又はマルチキャストドライバは單一のVLANに制限される。

【0 0 2 8】

また、本明細書においてVLANは「ノードマトリクル回報通信ドメイン」即ちVBDと称される。VBDは、ネットワークにおいて必ずしも物理的な接続（例えば、ケーブル）の変更の必要なしに規定され得る回報通信ドメインである。

【0 0 2 9】

管理端末 1 2 4 M には、プログラムやデータを記憶するための記憶装置 1 9 2 、並びにキーボード、スクリーン、及び／又は他のインターフェース機器のようなユーザインターフェース機器 1 9 4 が含まれる。

【0 0 3 0】

付録 B は、幾つかの実施例における接続グループを生成する（特に、VLAN 1 4 0 及びルータアクセス制御リストを生成する）プロセスを示している。ここで、このプロセスは図 1 の VLAN の例に示しており、また 3 つの接続グループは以下の通りである。

【0 0 3 1】

グループ1は、VLAN140a、140d、及び140bからなる。

【0032】

グループ2は、VLAN140b、140e、及び140hからなる。
(このグループは、管理端末124Mを含む管理接続グループとして指定され得る。)

グループ3は、VLAN140c、140f、及び140iからなる。

【0033】

幾つかの実施例においては、第2層ドメイン116Sは間報通信ドメインである。付録Bのプロセスは、ドメイン116Sを、任意の接続グループとの通信を許可された共用IPサブネットとして構成する。重要なことは、各第2層間報通信ドメインが、IPサブネット又はIPサブネットの組合せであることである。

【0034】

付録Bのプロセスは、第2層ドメイン116T及び関連するサブネットを「非管理(Managed)」状態にする(即ち、対応するルータインフェースに対してACLが生成されず、更にプロセスによって生成された任意のACLにおいてサブネット116Tは明示されない。)。従って、ドメイン116Tは任意の接続グループからトラフィックを受取り可能であるが、ドメイン116Tから任意の接続グループへのトラフィックは、ルータ130によって取除かれ得る(遮断され得る)。

【0035】

幾つかの実施例において、車……の第2層ドメインには、管理されたサブネット及び非管理のサブネットが含まれる。

【0036】

付録Bのプロセスは、任意のVLAN又は接続グループがネットワーク110において確立される前か或いは確立された後に実施され得る。幾つかの実施例において、付録Bプロセスが最初に実施され、全てのドメイン116(場合によって、ドメイン116S、116Tのような共用ドメイン及び非管理のドメインのエンティティを除く)における全ての通信エンティティを含む单一の「管理接続グループ(management connectivity group)」を確立する。その管理グループによつ

(17) て、管理端末1.2.4Mが全てのスイッチ及びルータと通信可能となる。次に付録Bプロセス又は付録Gのメントナンスプロセスが実施され、前述のグループ1、2、3又は別の任意のグループを確定する。そのようなグループの設置は、管理端末がスイッチ及びルータと通信する能力によって容易となる。

【0037】

戻りは、管理端末1.2.4M及びスイッチ1.2.8のポートのみが管理接続グループに配置される。幾つかの実施例においては、スイッチ1.2.8のそれらのポートのみが管理接続グループに配置され、その管理接続グループは管理端末1.2.4Mを全てのVLAN-capableスイッチ及び全てのルータと通信可能とすることを要求される。

【0038】

後述する実施例においては、付録Bプロセスの開始時に接続グループが存在しないと假定する。

【0039】

付録Bのプロセスが開始される前に、各ルータ1.3.0が構成されて、以上のIPサブネットが各ルータインターフェース2.1.0に割当てられる(図12)。(Cisco社の説明書において「サブインターフェース」と称される幾つかに對して、ここでは用語「インターフェース」を用いることに注意されたい。)付録Bのプロセスが完了した後に、各ルータ1.3.0は、それらが接続されるドメイン1.1.6の各VLAN1.4.0に対して個別のインターフェースを有し得る。

【0040】

各VLAN1.4.0はサブネット又はサブネットの組合せであるので、経路指定メントウェアがVLANを明確に認識しない場合でも、ルータ1.3.0がVLANに基づき事実上の送信決定を行うことに注意されたい。ルータは、ルータのトランクポート(例えば、トランクポート2.2.0)経由でドメインに接続され、また各インターフェースはトランクポートの論理的サブポートである。

【0041】

周知の通り、ルータ及びスイッチのトランクポート(即ち、スイッチ、又はスイッチ及びルータと相互接続するトランク1.5.0に接続されたポート)は、マル

チップVLANのためのトラフィックを通す。トランクポートにおけるトラフィックはトランクプロトコル（trunking protocol）を使用し、そこで各パケットは、パケットが割当てられるVLANの識別子を標識したよりも大きなパケットにカプセル化（encapsulated）される。VLANメンバーシップがMACアドレスよりも多くのポートによって規定される場合、VLANの標識によって受信スイッチ128がパケットのVLANを識別することが可能となる。

【0042】

ルータ130はトランクプロトコルを理解し、同一のトランクポートにおける種々のVLANからのトラフィックを、各VLANからのトラフィックがVLANに割当てられた個別のポートに到達した場合のように取り扱う。

【0043】

幾つかの実施例においては、トランクの代わりにルータと第2層ドメインとの間の個別の物理的接続を用いて個々のVLANに対するトラフィックを選ぶ。

【0044】

各インターフェースは、インターフェースによって取扱われる各サブネットにおけるゲートウェイアドレスを有する。ゲートウェイアドレスは、サブネットにおけるルータのアドレスである。

【0045】

付録Cは、記憶装置192において付録Bの幾つかのステップによって作成されたデータベースを示す。

【0046】

ステップM5（付録B）において、ネットワーク管理者は、管理端末124Mにネットワーク110のIPアドレスレンジを与える。付録Bの例において、アドレスレンジは10.0.0.0/8である。ネットワーク110において、各サブネットは255.255.255.0のサブネットマスクを有する。

【0047】

IPアドレスレンジ及びサブネットは、形式10.0.0.0/8（サブネットマスクは、全て0が続く有効な8つの1を有するか、或いはIPアドレス（10.0.0.0）及びネットマスク（255.0.0.0）の組合せのような形式を有する。

【0048】

付録Cの11に示すように、管理端末124Mはネットワーク110のIPアドレスレンジをそのデータベースに入力する。

【0049】

付録Bに示すように、ステップM7が管理者によって実施される。端末124Mがデータ構造12を生成する（付録C）。この情報及び付録Cにおける他の情報は、異なる実施例においては異なって編成される。例えば、幾つかの実施例において、項目12-1（スイッチのアドレス）は、各ドメインに対するアドレスのリストとして格納される。別の実施例においては、間接の情報は、アドレス及び各ドメインのペアとして格納される。別の実施例においては他のデータ構造が用いられる。

【0050】

ステップM10において、ネットワーク管理者がVLAN1-40を規定する。VLANの規定には、各ドメイン1-16における各スイッチ128及び端末124Mに対してVLAN識別子を与える過程が含まれる。VLAN識別子は、スイッチ128に認識可能な識別子（即ち、VLAN番号）である。例えば、スイッチ128-1、128-2の各々は、VLAN1-40a、1-40b、1-40cの識別子を受信し、スイッチ128-7は、VLAN1-40g、1-40h、1-40iの識別子を受信する。VLANを規定する過程には、何れのエンティティ（ポート、MACアドレス又はエーチ名）が各々のVLANに属するかを明らかにする過程は含まれない。

【0051】

既存実施例においては、管理者がVLAN識別子を各スイッチ128に直接入力する。別の実施例においては、管理者がVLAN識別子を各ドメイン1-16の制御スイッチ128に入力する。制御スイッチは、同一のドメインにおける別のスイッチ（仮に存在すれば）に対して識別子を送信する。更に別の実施例においては、管理者はこの情報を例えばTelnet又はSNMPプロトコルを用いて端末124Mから遠隔のスイッチ128に情報を与える。

【0052】

付録Cの13に示すように、端末124Mはこの情報をそのデータベースに入力する。

納する。

【〇〇53】

ステップM1.4において、ネットワーク管理者は情報1.4(付録C)を端末1～4Mに入力する。図1及び図2において、個々のサブネットは各第2層BDに割当てられ、第2層BDとIPサブネットとの間に1対1対応が存在する。サブネットは、図2及び次の表1に示されている。

【〇〇54】

【表1】

表1

第2層BD	サブネット
140a	10.1.1.0/24
140b	10.1.2.0/24
140c	10.1.3.0/24
140d	10.2.1.0/24
140e	10.2.2.0/24
140f	10.2.3.0/24
140g	10.3.1.0/24
140h	10.3.2.0/24
140i	10.3.3.0/24
116s	10.3.4.0/24
116t	10.2.4.0/24

【〇〇55】

幾つかの実施例においては、複数のサブネットが第2層BDに付して割当てられている。

【〇〇56】

サブネットは、サブネットマスクの表記法、又はサブネットアドレス及びマスクの表記法における1のサブネットアドレス／番号を用いて端末1～4Mに与えられる。

【0057】

またステップM1.4において、対応するIPサブネットから各VLANにおけるIPアドレスを割当するためにネットワーク1.0が機械化される。従って、幾つかのWindows NTTMの実施例において、DHCPサーバーは各サブネットにおいてIPアドレスを割当てるために構成される。(Windows NTについては、例えば、Sant' Angeloの“Windows NT Server Survival Guide”(1996)に記載されており、これについては、ここで省及することにより本明細書の一部とする。)幾つかの実施例においては、DHCPリクエストをルータに直接送信された全てのサブネットから。ルータは、DHCPのリクエストをルータに直接送信された全てのサブネットから。のDHCPサーバへ送信するよう構成される。別の実施例においては、個別のDHCPサーバが各サブネットに設けられる。

【0058】

ステップM2.0において、各接続グループに対して、管理者は接続グループのメンバであるIPサブネット(即ち、接続グループのメンバである第2層BDの一部であるIPサブネット)を端末1.2.4.Mに入力する。従って、管理者は、接続グループに対してVLAN 1.4.0.a、1.4.0.d、1.4.0.gににおけるサブネットを入力し、グループ2に対してVLAN 1.4.0.b、1.4.0.e、1.4.0.hににおけるサブネットを入力し、更にグループ3に対してVLAN 1.4.0.c、1.4.0.f、1.4.0.iにおけるサブネットを入力する。或いは、各接続グループに對して、管理者は、接続グループの第2層BDメンバの識別子を入力する。各々のケースにおいて、全てのルータを管理端末1.2.4.Mから到達可能とするために、管理者は、管理接続グループのメンバであるIPサブネットを入力し得る。幾つかの実施例において、各ルータは、共有サブネット又は管理接続グループのサブネットメンバにおける少なくとも一つのゲートウェイIPアドレスを有する。

【0059】

幾つかの実施例では、全てのルータが管理端末から到達可能であることを必要としない。従って、管理者でないサブネット及び他のルータにのみ直接接続されたルータは、幾つかの実施例においては到達可能であることを必要としない。

【00601】

項目15（付録C）が、ステップM20において生成される。

【00611】

多數のサブネットが単一の第2層BDに割当された場合、それらは全て同じ接続グルーブに割当られる。

【00621】

ステップM30において、管理者が各接続グルーブに属するエンティティを端末124Mに入力する。ここで、16（付録C）が生成される。例えば、接続グルーブ1の場合、管理者はスイッチポート160.1、160.2、160.3（ポート160.3に接続された端末124.3はVLAN1.4に属すると仮定する）、及び他のポート、MACアドレス、並びに／又はVLAN1.40d、1.40a、1.40d、1.40aに属するユニーク名を入力する。幾つかの実例においては、管理者は、ポート、MACアドレス又はユニーク名がどのドメイン又はVLANに属するかを記憶する必要がない。

【00631】

ポート160は、参照が容易なように管理者によって割付けられるレベルによつて、端末124Mにおいて識別される。例えば、ポートがユニーク名Fredのユニークによって使用される端末124に接続されている場合、管理者はそのポートにラベル「Fred」を割付けることができ、またステップM30において「Fred」を入力してこのポートを接続グルーブに割付けることが可能である。MACアドレスの接続グルーブへの割付けも同様である。

【00641】

ステップM40において、管理者は情報を17及び18（付録C）を管理端末124Mに入力する。

【00651】

ステップM45において、端末124MがVLAN1.40を生成し、付録Dに示すように各エンティティを適当なVLANに配置する。付録Dにおいて、括弧内の番号は、付録Dの対応するステップにおいて用いられる付録Cのデータベース項目を指す。

【00661】

【0067】

同様に、ユーチャ名が接続グループの全てのVLAN1.4.Oに配置される。ユーチャがドメイン1.1.6.Pにロダオンした場合、ユーチャが適切なVLANに切替えるためにUBNCサーバー間に存在する要挟がドメイン1.1.6.Pから届く。例えばUBNCサーバーはどのVLANがどの接続グループに存在する場合、UBNCサーバーはユーチャをVLAN1.4.Oに配置する。同様に、ユーチャがドメイン1.1.6.Q又は1.1.6.Rにロダオンする場合、UBNCサーバーは、ユーチャをVLAN1.4.O又は1.4.Oにそれぞれ配置する。

【0068】

ステップV3において、「実施例1.1.1は接続グループに関連する任意の事項を知るためにUBNCサーバーを必要としない。端末1.2.4.Mは、各ドメイン1.1.6におけるユーチャ名に対してもVLANが割当てられるかをUBNCサーバーに知らせる（ステップV3-2）。実施例2においては、UBNCサーバーはどのVLANがどの接続グループに属するかを認識している（この情報はUBNCサーバーが直接与えられるか、或いは例えば端末1.2.4.Mから遠隔的に与えられる）。従つて、実施例2のステップV3-1に於いて、端末1.2.4.MはどのVLANがユーチャに割当てられるかをUBNCサーバーに通知しない。ユーチャがロダオンした時、UBNCサーバーはロダオンが生じた

ドメイン1.1.6及びユーパークの接続グループからユーパークのVLANを決定する。UBNCデータベースには、各ドメイン1.1.6における各VLANに關連するIPサブネットが含まれるので、ドメイン1.1.6はユーパークのIPアドレスから決定される。幾つかの実施例においては、UBACナーバは管理端末1.2.4.Mにおいて作動する。

【0069】

ステップM5.0(付録B)において、端末1.2.4.Mは、付録Eにおけるプログラムを実行することによって、ルータアクセス制御リストを作成する。個別のアクセス制御リストが、接続グループのサブネット番号が直接結合付けられる各ルータインターフェースに対して作成される。付録Eのプログラムは、ルータ130.2からVLAN140.0までのインターフェース210の例において説明され得る。

【0070】

各ルータインターフェースに対して、対応するサブネットが所定の接続グループに属する場合、付録Fに示すようにステップA1からA5によってアクセス制御リストが作成される。付録Fにおける回線番号(例えば、A.L1-1)は、付録Eのステップ番号に對応する。従って、例えばステップA1(付録E)は回線A.L1-1を生成し、ステップA2は回線A.L1-2.a及びA.L1-2.bを生成する。

【0071】

付録Fは、Cisco社(San Jose, California)の幾つかのルータによつて用いられるシンタクスを用いる。このシンタクスについては、K. Siyan及びC. Hareの“Internet Firewalls and Network Security”(1995), 186-191頁に記載されており、これについてはここで省略することにより本明細書の一部とする。回線番号(例えばA.L1-1)は、アクセス制御リストの一部ではない。更に、感嘆符(!)で始まり行の終わりまで絶く文義は、ルータによって無視されるコメントである。これらのコメントは幾つかの実施例においては省略される。

【0072】

ステップA1は、サブネット1.1.6.Sのような各共用サブネットからのインタフェース210へのトライックを許可する回線を生成する。そのプログラムは、アクセス制御リストに対して、「アクセスリスト(access-list)」、アクセス

制御リスト番号（幾つかの実施例においてプログラム自身によつて連続的に発生する）、「許可 ip (permit ip)」、共用サブネットのIPアドレス、並びに0.0.0.255のワイルドカードマスクを書き込む。（入力のパケットIPと比較して、ワイルドカードマスクにおける0ビットは、発信元IPアドレスの対応するビットがルータによって使用されていることを示し、ワイルドカードマスクにおける1ビットは、対応するビットが使用されていないことを示す。）
回線A L1—1におけるワイルドカードマスク0.0.0.255は、サブネットマスクを反転させることによって決定される。）

【0073】

ステップA2は、同一の接続グループにおける他の全てのサブネット（即ち、第2層 BD）からのトラフィックを許容する（例えば回線A L1—2 a、A L1—2 bのような回線を生成する。回線A L1—2 aは、サブネット10.1.2.0/24 (VLAN 1.40 b) からのトラフィックを許容する。回線A L1—2 bは、サブネット10.3.2.0/24 (VLAN 1.40 h) からのトラフィックを許容する。）

【0074】

ステップA3は、ネットワーク110における他の全ての端末からのトラフィックを拒否する回線A L1—3を生成する。（重要なことは、ルータがパケットを受取ったときに、ルータがアクセス制御リストの始まりからパケットの開始をデストすることである。パケットに適合する行が発見されたとき、アクセス制御リストの残りの部分は無視される。）ワイルドカードマスクは、ネットワーク110のIPアドレスレンジマスクを反映させることによって得られる。

【0075】

ステップA4によって、インターネット170からのトラフィックを含むネットワーク110の外部の任意の端末からのトラフィックを許容する回線A L1—4が生成される。

【0076】

幾つかの実施例において、管理者は、ステップM 50の前に接続グループにおける各サブネットに対する、インターネットからサブネットへのトラフィックが許可されるかどうかを管理端末1.2.4 Mに示す。トラフィックが拒否された場合

は、対応するインターフェースに対してステップA4が省略され、またステップA3がラインA L 1 - 3の代わりの「任意の拒否ip (deny ip any)」固線を生成する。

【0077】

付録Eに示すようにステップA5が実施される。

【0078】

ルータインターフェースが後続ループのBDシノユニットに接続されずに、共用者として接続されることは非管理サブネット（例えば1.6.0.0/S）又はインターネット170に接続される場合、ACUは生成されずにサブネット群しくはインターネットは他の任意のサブネットからアクセス可能となる。

【0079】

幾つかの実施例においては、付録BのステップM40において、管理者は各共用サブネットに対してどのようなアクセスが与えられるかを指定し、付録Eのブロセスによって、当該端に閑知の方法を用いて適切なアクセス制御リストを作成される。例えば、共用サブネットがネットワーク1.1.0の子からのみアクセス可能となる場合、アクセス制御リストは以下のよう構成され得る。

【0080】

アクセスリスト1許可ip 10.0.0.0 0.255.255.255

アクセスリスト1拒否ip 任意

別の実施例において、どのような機能性は、ルータ130.1又は他の幾つかの機器（図示せず）において実現される企業会社に応じて以下のように構成されて与えられる。

【0081】

管理端末1.2.4Mは、存在する全てのアクセス制御リストを消去して、新しいアクセス制御リストに置き換えるように各ルータ130に指示する。

【0082】

幾つかの実施例においては、ネットワーク管理者は追加のコマンドをアクセス制御リストに挿入することが可能である。従って、幾つかの実施例においては、管理者が、ステップM50の前に対応するインターフェースに対してアクセス制御

リストに挿入される各サブネットの追加項目を指定し得る。詳述すると、管理者は、ステップA 1 の前に挿入される項目、ステップA 2 とA 3 の間で挿入される項目、ステップA 3 とA 4 の間に挿入される項目、及びステップA 4 の後に挿入される項目を指定することができます。幾つかの実施例において、この技術を用いてファイアウォールの機能をアクセス制御リストに組みみ、従つて、企業全体に渡る個別のファイアウォールの必要なくなる。

【0083】

幾つかの実施例においては、ステップM 1 0 及びM 2 0 が省略される。ステップM 4 5において、各接続グループに対して、管理端末1 2 4 Mは、VLAN…capableスイッチ及び接続グループに付与する各ドメイン1 1 6 においてVLANを生成し、またVLANにエンドティティを配置する。(従つて、ドメインが接続グループにおけるポート1 1 6 0 を有する場合、或いは接続グループにMACアドレス又はユーザ名が含まれる場合には、VLANがドメインの中に生成される。) また端末1 2 4 Mによって、IPサブネット(例えば、10.1.1.0/24) がVLANに割り当てられる。

【0084】

幾つかの実施例においては、VLANのメンバーシップは、ポート、MACアドレス又はユーザ名以外の他の標準によって決定される。従つて、幾つかの実施例においては、VLANのメンバーシップは、例えば第2層パケットにおけるビットの値のようなパケットの内容に基づき決定される。スイッチ1 2 8 が、以上の値の予め決定されたセットの中にそのようなビットの値が存在するパケットを受取るとき、そのスイッチは、パケットの発信元MACアドレス、又はパケットが到達するポート1 1 6 0 を検応するVLANに配置する。スイッチ1 2 8 はパケットに挿入されたトランクポートにおけるパケットを透かす場合、スイッチはパケットにパケットのVLAN番号を付加する。ルータ1 3 0 において、各VLAN番号はインターフェースに関連するものである。(この関係は、インターフェースが規定されたときに確立される。) 従つて、図2に示すように、各ルータ1 3 0 は、そのルータが直接接続される各IPサブネットに対する個別のインターフェース2 1 0 を有する。付録B～Gの実施例と同様に接続グループが生成される。特にステップM 3 0 に

において、管理者は、各接続グループに対して、どのようなパケットがその接続グループに属するかを决定するルールを指定する。例えば、所定のルールによって所定のビットの値を有するパケットが所定の接続グループに属することが決定され得る。

【0085】

幾つかの実施例においては、ルータ130におけるアクセス制御リストによつて、IPアドレスとは別の基準に基づきトラフィックを許可するか或いは拒否する。例えば、或る基準にはポート番号が関係する(例えば、W. Cheswick及びS. B. Howinの“Firewalls and Internet Security”(1994), 94-109頁を参照；ここで普及することにより本明細書の一部とする)。更に、所定の基準によつて、インターフェースへのトラフィックよりも寧ろインターフェースからのトラフィックを指定する。管理者は、ステップM50の前に端末124Mに対して十分な情報を与え、そのような基準に従つてアクセス制御リストを作成する。

【0086】

幾つかの実施例においては、冗長(redundancy)を目的として、VLAN140が間のルータの異なるインターフェース210に接続され得る。2つのインターフェースは、同一のサブネットか或いは2つの異なるサブネットに割当てられる。各ACLは、両方のインターフェースに対して同様の制限を与える。

【0087】

VLANが複数のルータのインターフェースに接続されるとき、場合によっては別のルータからアクセス可能な別の端末への情報の経路を指定するためには、ルータの1つがVLANを経由して別のルータへデータを送信することを試みることができる。その場合、VLANに接続されたインターフェースに対するACLが、ルータ間のトラフィックを過度に制限しないように構築される。幾つかの実施例においては、VLANサブネットは共用されるか或いは非管理であり、任意の接続グループのメンバではない。

【0088】

付録Gは、ネットワーク110において接続性を変更するためのメンテナンスプロセスを示す。付録Bのプロセスの実施数行によつて、任意の変更を行うことが

可能である。しかしながら、幾つかの実施例において付録 C プロセスがメンテナансを容易にする。

【0089】

幾つかの実施例において、ステップ M50 は省略される (ACI は生じない)。

【0090】

前述の実施例は本発明を限定するものではない。本発明は、特定のネットワーク、層、スイッチ、ルータ、オペレーティングシステム、成いは他のノードウェア若しくはソフトウェアに限定されるものではない。また本発明は企業ネットワークに限定されるものではない。幾つかの実施例においては、MAC アドレスは NIC に書き込まれるものではなく、ソフトウェアによって生じる。幾つかの実施例において、付録 B-1 G の管理ソフトウェアの全て或いはその一部は端末 124 より繋るスイッチ 128 又はルータ 130 で実行される。ソフトウェアは幾つかの実施例に適用される。

【0091】

幾つかの実施例においては、ドメイン 116 は第2層プロトコルとは別の中継トコルを使用し、ルータ 130 は、第3層プロトコルとは別の中継トコルに基づきトラフィックの絶路選択を行う。各ドメインにおける接続性は、MAC アドレス又は第2層ハンドセットの内容とは別的情報に基づき決定され、ルータ 130 は、IP アドレスとは別的情報に基づきトラフィックを許容又は拒否する。幾つかの実施例においては、ルータ 130 は IPX アドレスを使用する。幾つかの実施例においては、D. Bierer らの "NetWare 4 for Professionals" (1993) (ここで省及することにより本明細書の一部とする) に記載のネットワーク若しくはブレトルーフネットワークを使用する。他の実施例及び後述例は、添付した請求の範囲によつて規定される本発明の範囲内である。

付録 A

ユーザ→ネットワークコントロール (UBNC)

幾つかの実施例において、VLAN のメンバーシップは端末にログオンしたユーザに基づき決定される。Windows NTTM の幾つかの実施例においては、UBNC がすべての VLAN からアクセス可能なよう設置される (例えは、サーバが直接サブネット

ット内にある）。ネットワーク端末が能力アップされた(powered up)とき、それは「デフォルト(default) VLANに配置される（デフォルトVLANは各々の第2層ドメイン11.6に存在する）。端末は、デフォルトVLANを提供するDHCPサーバーからIPアドレスを受取る。ユーザが端末にログオンした時、端末はUBNCサーバーにに対して、ログオン時に与えられたユーザ名に属するVLANに端末を切替えるよう必要を送る。その要求には、ユーザ名、端末のMACアドレス、及び端末の現在のIPアドレスが含まれる。UBNCサーバーは、UBNCサーバーへベースから関連するVLANを決定する。或る実施例においては、各ユーザ名に対して、データベースには関連するVLANの識別子が含まれる。別の実施例においては、データベースには管理端末によって与えられる以下のような情報が含まれる。

【0092】

(A) 各ユーザ名について、そのユーザ名が属する接続グループの識別子

(B) 各接続グループに属するVLANの識別子

(C) 各VLANについて、関連するサブネット

UBNCサーバーが要求を受取ると、サーバは要求する端末に対しても（1）端末が異なるVLANに切替えられるかどうかの指示（端末がデフォルトVLANになら、ときにユーザがログオンした場合、切替が要求されない可能性があり、またVLANが規定されていないレイヤ2 BDにユーザがログオンした場合、切替が行われない可能性がある。）、並びに（2）ユーザに割当てられたVLANのIPサブネット及びサブネットマスクを送信する。次にUBNCサーバーは、端末がそのDHCPリース(DHCP lease)を解放するのを待つ。そこでUBNCサーバーは、端末を含む第2層ドメイン1.1.6における单一のスイッチ又は複数のスイッチ1.2.8に対して適切なエマンドを送信する。そのスイッチによって、ユーザに割当てられたVLANに端末が配置される。

【0093】

UBNCサーバーから応答を受取った後に、端末はそのDHCPリースを解放し、次にユーザへIPが端末を割当てられたVLANに切替え可能なように所定の期間待つ。その期間の後に、端末は切替が完了したと想定し、新たなIPアドレスの要求を送出する。応答において、端末は新たなIPアドレスを受取る。端末は新たなIPをUBNCサーバーから受取ったサブネットマスク及びIPサブネットと照合する。新たなIPがサブ

ネットに存在しない場合、端末は新たな要求をUBNCチャーブに対して送出することによってその手続きを繰り返す。端末が新たなIPを要求したときに端末が割当てられたVLANに切替えられる。新たなIPは割当ったサブネットに存在する可能性がある。

【0094】

幾つかの実施例においては、デフォルトVLANは省略される。別の実施例においては、全ての端末又は地理的にもっとも近い端末のグルーブが個別のデフォルトVLANに割当てられ、UBNCチャーブによってユーザがそれらと関連するVLANに切替えられるまで通信を制限する。ユーザがログオフした時、ユーザ端末は適切なデフォルトVLANに戻される。

付録B

接続グループ(Connectivity Groups)の生成

M.5. 管理端末124Mにネットワーク110のIPアドレスレンジ(例えば、10.0.0.8)を与える。

M.6. 管理端末124Mに構編12(付録C)を与える。

M.1.0. VLANを定義する。

M.1.4. 第32層BDにIPサブネットを割当てる。

M.2.0. 各接続グループに対し、管理端末にグルーブのIPサブネットメンバを与える。1つの接続グループを管理接続グループとして指定する。

M.3.0. 接続グループに管理可能なエンティティ(ポート、MACアドレス及びユーザ名)を割当てる。

M.4.0. 管理端末に情報17及び18を与える。

M.4.5. 管理端末124Mが、エンティティを適切なVLANに配置する(付録D参照)。

M.5.0. 管理端末124Mが、ルータのためのアクセス制御リストを作成する(付録E参照)。

付録C

管理端末データベース

1.1. ネットワーク110のIPアドレスレンジ

1.2. 各ドメイン116について

1.2.1. ドメイン116における全てのVLAN—capableスイッチ128

のIPアドレス

1.2.2. 各スイッチのポートランクがト160の識別子

1.3. 各ドメイン116について、ドメインにおけるVLANの識別子

1.4. 各第2層BDにについて、BDがVLANであるか否か、またIPサブネットがBDに含まれているか否かの指示。BDがVLANである場合、VLANの識別子。

1.5. 各接続グループについて、その接続グループに属するIPサブネット

1.6. 各接続グループについて、その接続グループに属するエンティティポート、MACアドレス、及び／又はユーネーム名

1.7. 各ルータインターフェースについて

1.7.1. 開通するサブネット（仮に存在せず）

1.7.2. インタフェースがVLAN—capable第2層ドメインに接続されているか否かを指示するフラグ

1.8. ネットワーク110における全ての共用サブネットのリスト

付録D.

VLANの生成各接続グループCGについて、また接続グループにおける各エンティティポート160

について、

V.1. エンティティEがVLAN—capableスイッチ128のポート160である場合、

V.1.1. ポートが属するドメイン116—E（116P、116Q、1

116Rの1つ）を検索する（12—2、12—1）

V.1.2. 接続グループCG及びドメイン116—Eの両方ににおけるVLANを検索する（13、14、15）

V.1.3. ドメイン116—Eのスイッチ128又はドメイン116—Eの制御スイッチ128に対してコマンドを送信することによってポートEをVLANに配置する

V.2. 戻りはエンティティEがMACアドレスである場合、接続グループCGにおける

る各VLANについて (14、15)、

V.2—1. VLANを含むドメイン116—V (116T、116Q、116Rの1つ) を決定する (13)

V.2—2. ドメイン116—Vの制御スイッチ128又は全てのスイッチ128に対して適切なコマンドを送信することによってMACアドレスE5 VLANを配置する

V.3. 戦いはエンティティEがユーネ名である場合、

実施例1：接続グループCCGにおける各VLANについて (14、15)、

V.3—1. VLAN (13) を含むドメイン116—Vを決定する

V.3—2. VLAN識別子、ドメイン116—Vの識別子、及びユーネ名をUBNCサーバーにに対して送信する

実施例2：

V.3—1. 接続グループCCGの識別子及びユーネ名をUBNCサーバーに送信する

付録E

ステップM.5.0：リンクエストに対するアクセス制御リストの生成

ネットワーク110における各ルータについて (12—3)、またルータの各インターフェースについて (17)、インターフェースと接続されたサブネットが接続グループに属する場合、

A.1. 各其のサブネットからのトラフィックを許可する (18)

A.2. 同一の接続グループにおける全てのサブネットからのトラフィックを許可する (15、14)

A.3. ネットワーク110における他の全てのサブネットからのトラフィックを拒否する (11)

A.4. ネットワーク110の外部からのトラフィックを許可する

A.5. ルータにおいてTelnetセッションを開放し、ルータに対して以下を送信する

(1) インタフェースから存在するACL (もし存在すれば) を削除くためのコマンド (例えは、非アクセスグループ1)

(2) アクセスリスト

(3) ゴマンド:

interface vlan_e

これからのコマンドにより、ACLが「vlan_e」と標識されたルータインターフェースに對して割当られる
付録F

vlan_4_0_eに対するルータインターフェース2.1.0のためのアクセス制御リスト上

ACL_1_1_1 アクセスリスト1番番号 10.3.4.0 0.0.0.255
! 共用サブネット

ACL_1_1_2_a アクセスリスト1番番号 10.1.2.0 0.0.0.255
! 同一のものにおけるサブネット
! 企業の接続グループ

ACL_1_1_2_b アクセスリスト1番番号 10.3.2.0 0.0.0.255
! 同一のものにおけるサブネット
! 企業接続グループ

ACL_1_1_3 アクセスリスト1番番号 10.0.0.0 0.255.255.255
! ネットワーク1.1.0における全てのサブネット
! 同一の接続グループの外部

ACL_1_1_4 アクセスリスト1番番号 任選
! からのアクセスの許可
! ネットワーク1.1.0の外部

付録G

メンテナンスアルゴリズム

非管理から接続グループのメンバへのサブネットの変更
サブネットが1以上のデータウェイアドレスを有する場合、サブネットは接続
グループのメンバに変更されない。そもそもれば、サブネットを接続グループ…ブに
付加し、付録Eに示すように、同一の接続グループにおけるサブネットが直接接
続される日々のインスタンスに対するアクセス制御リストを再生成する。

共用サブネットのリスト 18 (付録 C) にサブネットを付加する。付録 E に示すように、任意の接続グループにおけるサブネットが継続される各ルータインターフェースのアクセス制御リストを再生成する。(サブネットは各 ACL に付加され得る。)

共用から非管理へのサブネットの変更

共用サブネットのリスト 18 (付録 C) からサブネットを除去する。付録 E に示すように、任意の接続グループにおけるサブネットが継続される各ルータインターフェースのアクセス制御リストを再生成する。(サブネットは各 ACL から除去され得る。)

接続グループのメンバから非管理へのサブネットの変更

サブネットが 1 を越えるゲートウェイアドレスを有する場合、サブネットは接続グループのメンバに変更されない。さもなければ、サブネットを其用サブネット (付録 C) のリスト 18 から除去し、新たにサブネットを接続グループ (付録 C における 14) に付加する。付録 E に示すように、任意の接続グループ...アににおけるサブネットが継続される各ルータインターフェースのアクセス制御リストを再生成する。

接続グループのメンバから非管理へのサブネットの変更

接続グループ (付録 C の 15) からサブネットを除去する。付録 E に示すように、同一の接続グループ...アにおけるサブネットが直接接続される各ルータインターフェースのアクセス制御リストを再生成する。(サブネットは各 ACL から除去され得る。) 付録 E に示すように、サブネットは直接接続されたルータインターフェースに対する ACL を除去し、次に (必要なら) 再生成する。(インターフェースに直接接続された他のサブネットが存在しない場合は、ACL は生成されない。別の單一のサブネット又は複数のサブネットが存在する場合は、適切な ACL が生成される。)

接続グループのメンバから其用へのサブネットの変更

接続グループ (付録 C における 15) からサブネットを除去する。サブネットが直接接続されているルータインターフェースに対する ACL を除去する。付録 E に示すように、任意の接続グループにおけるサブネットが直接接続されている各ルータ

ータインタフェースのアクセス制御リストを再生成する。(サブネットは、グルーブのメンバとして幾つかのACLから取除かれるが、共用サブネットとして各ACLに付加される。)

1つの接続グルーブ（「旧」グルーブ）から別のグルーブ（「新」グルーブ）へのサブネットの移行

サブネットを旧グルーブから取除き、新グルーブ（付録Cの15）に付加する。付録Eに示すように、古い又は新規の接続グルーブの何れかにおけるサブネットが直接接続された各ルータインタフェースのACLを再生成する。

接続グルーブへの直置エンティティ（ポート、MACアドレス、ユーザサブ）の付加
（ステップM.3.0参照）

管理者は、新しいエンティティが属すべき接続グルーブを指示する。

【0095】

ポート1.6.0 ポートはスイッチ1.2.8に接続され、それはそれ自体が第2層ドメイン1.1.6の一部である。所定の第2層ドメインにおいて、選択された接続グルーブは特定のサブネットと接続され、それは、それ自体が特定のVLANと結合される。ポートが接続グルーブに割り当てられる際に、ステップV.1（付録D）が実行され、ポートが第2層ドメインにおける接続グルーブのメンバであるVLANに配置される。マルチポイントモジュールがスイッチに付加される場合のように、或いは全部のスイッチがネットワークに付加される場合のように、通常はポートがグルーブに付加されることに注意されたい。これらの場合において、新しいポートの全てのセットが、管理者によって選択された接続グルーブに付加される。次に（もし必要ならば）管理者は1つずつポートの割当を変更することができる。

【0096】

MACアドレス ポートに関する場合のように、特定の第2層ドメインにおいて、選択された接続グルーブがサブネット/VLANペアに接続される。各第2層ドメインに対して、ステップV.2（付録D）によって、所定のMACアドレスが指定されたVLANに割当られるように、全てのスイッチ（又はスイッチの能力次第で、单一の御制スイッチ）が形成される。

【0097】

2.4.3 付録DのステップV3を参照。

或る接続グループ（「旧」グループから別のグループ（「新」グループへの通信エンドティエ（ID）、MACアドレス、ユーチャ）の移行（ステップM.3.0参照）

ポート1.6.O ポートはVLAN-capableスイッチ1.2.8に接続され、それはそれが自体が第2層ドメインの一部である。第2層ドメインにおいて、新旧の接続グループは特定のサブネットに接続され、それらは、それら自体が特定のVLANに結ばれる。新しい接続グループに属する第2層ドメインにおいてサブネットが存在しない場合、変更は行われない。）管理端末1.2.4.Mは、新しいVLANに対するポートの割当を変更する。

【OO98】

MACアドレスマートポートの場合のように、特定の第2層ドメインにおいて、新規の接続グループはサブネット／VLANペアに割当する。各第2層ドメインについて、所定のMACアドレスが指定されたVLANに割当てられるように、端末1.2.4.Mが全てのスイッチ（又はスイッチの能力が事で、单一の制御スイッチ）を構成する。特定の第2層ドメインにおける要求された接続グループに対応するサブネットが存在しない場合、第2層ドメインにおけるMACアドレスに対するVLANの割当は行わられない。移行の結果として、或いは第2層ドメインにブレイクインされたラップトップ又は他のモバイルコンピュータにMACアドレスが割当られるために、MACアドレスが第2層ドメインに生じた場合、そこでスイッチは未知のMACアドレスが発生したときに、それらが通常通り得る全ての動作をとり得る。

【OO99】

ユーチャ 付録DのステップV3を参照。

初期のルータインターフェース／VLAN／サブネットの付加
新規のルータインターフェース2.1.0が、直接接続されたサブネットを含まない場合（ゲートウェイアドレスがない場合）、動作は要求されない。さもなくば、インターフェースは以上のゲートウェイアドレス及び対応する直接接続されたサブネットを有する。直接接続された各サブネットについて、
1. サブネットが既に接続グループのメンバーである（従って、別のルータのイ

ンタフェースに直接接続されている)場合、サブネットは共用サブネットに変更される。前述の接続グループのメンバから共用サブネットへサブネットを変更するためのプロセスを参照されたい。

【O 1 0 0 1】

2、或いはサブネットが共用又は非管理として既に指定されている場合、動作は要請されない。

【O 1 0 1 1】

3、或いはサブネットは新規のサブネットである。サブネットを共用サブネットのリスト128(付録C)に付加する。付録Eに示すように、任意の接続グループにおけるサブネットが直接接続された各ルータインタフェースのアクセス制御リストを再生成する。(サブネットは共用サブネットとして各ACLに付加され得る。)サブネットがVLAN-capableスイッチ128を含む第2層ドメインに存在する場合、新規のVLANがドメインの中に生成され、新規のサブネットと接続される。

新規のルータの付加

新規のルータ130は幾つかのインタフェースを有し得る。各ルータインターフェースに対して、新規のルータインターフェースのためにリストされた動作が実行されれる。

新規のVLAN-capableスイッチの付加

新規のVLAN-capableスイッチ128が第2層ドメインに付加され、そこでは管理接続グループに割当てられたサブネットが存在し、またこのグループに対応するVLANが存在する。

【O 1 0 2 1】

スイッチが、ポートベースVLAN(port-based VLAN)を実現する場合、スイッチの管理スタッフ及びスイッチにおける全てのポートは、管理接続グループにおけるサブネットに割当てられる。更に、スイッチはこのサブネットからのIPアドレスに割当てられる。例えば、サブネット10.50.3.0/24が、管理グループに割当てられた第2層ドメインにおけるサブネットである場合、またVLAN3が、サブネット10.50.3.0/24に関連するVLANである場合、管理接続グループに

おけるアドレスに割当てるために、Cisco Catalyst 5000シリーズスイッチのコンソールにおいて次のようにコマンドを発行する。

【O 1 O 3】

```
set interface s0/0 3 10.50.3.200 255.255.255.0 10.50.3.255
ここでs0/0は、スイッチの管理スイッチに対する指名子であり、3は、サブネット10.50.3.0/24に対応するVLANであり、10.50.3.200は、スイッチの管理スタッフに割当てられたサブネット10.50.3.200/24におけるIPアドレスであり、255.255.0は、サブネット10.50.3.0/24に対するサブネットマスクであり、更に10.50.3.255は障害通信アドレスである。
```

【O 1 O 4】

スイッチがMACアドレスVLANを実現する場合、管理スタッフのMACアドレスは、管理後続グループにおけるサブネットに対応するVLANに割当てられる。ポートベースVLANの場合のように、スイッチはこのサブネットからのIPアドレスに割当てられる。

新規の接続グループの付加

新規の(2nd)接続グループは常に付加され得る。サブネットを接続グループにどのように付加するかについては前述の通りである。

【画面の簡単な説明】

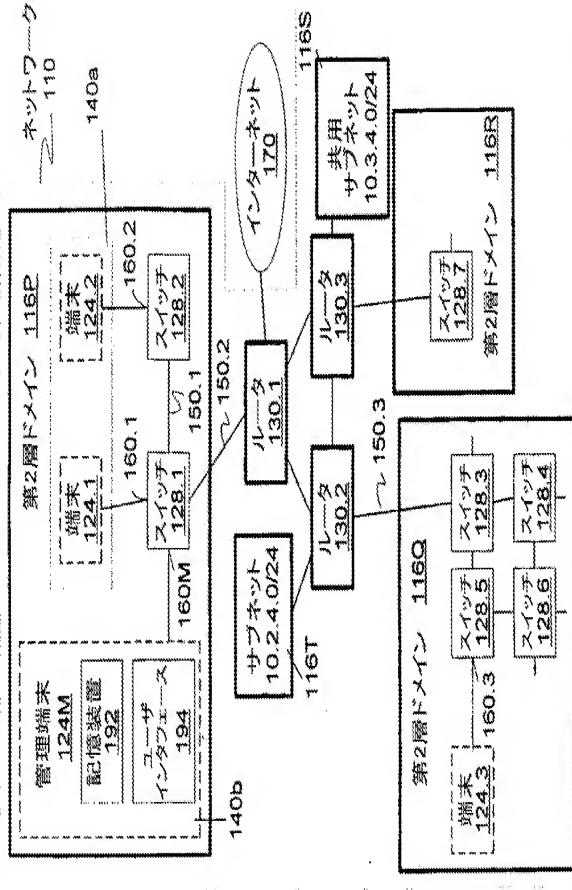
【図 1】

本発明により接続を確立したネットワークのプロック線図である。

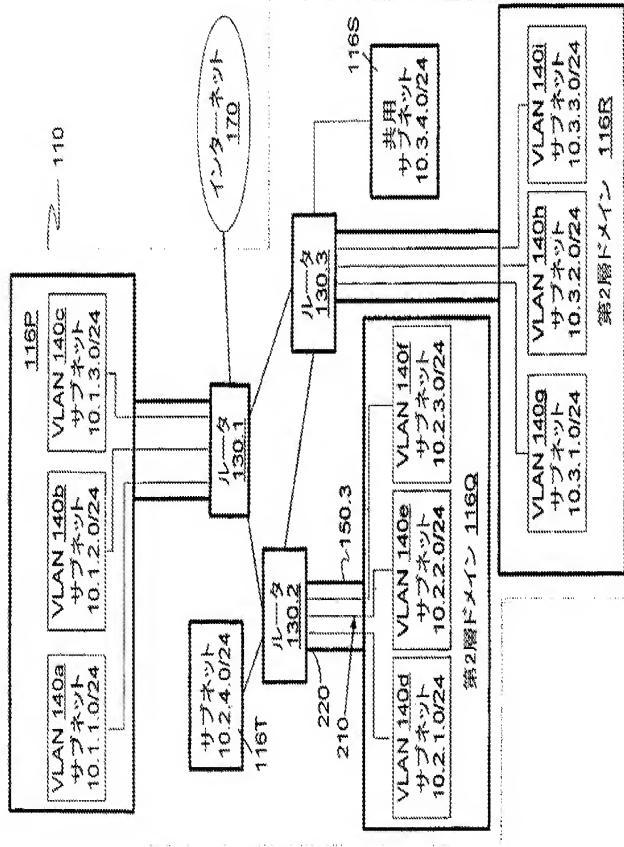
【図 2】

図1のネットワークにおけるVLAN及びルータインターフェースを示すプロック線図である。

【図1】



【図2】



【手続補正書】特許権力譲約第34条補正の翻訳文提出書

【提出日】平成12年4月12日(2000.4.12)

【手続補正】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】ネットワーク端末をノードチャラル間接通信ドメイン(VBDS:

140a乃至140i)に接続するための方法であつて、

ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から送信する過程と、
ユーザを識別する情報をからにして上のVBDSを含むユーザの属する接続グループを決定する過程と、
前記ネットワーク端末が接続される以上上のVBDSを決定する過程であつて、前記
1以上のVBDSが前記接続グループのメンバであるよう前記決定過程と、
前記ネットワーク端末を前記1以上のVBDSに接続するためのコマンドを発行する
過程とを含むことを特徴とする方法。

【請求項2】各VBDSが、前記トライックが生じる前記VBDSへの両報通側
トライックを制限可能なドメイン(116P)のサブドメインであり、
前記接続グループが、少なくとも2つのドメインからのVBDSを含み、
前記ネットワーク端末が接続された以上にVBDSが、前記ネットワーク端末を含
む前記ドメインに接続されることを特徴とする請求項1に記載の方法。

【請求項3】各VBDSがVLANであり、また前記ネットワーク端末が、前記
接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接
続されることを特徴とする請求項2に記載の方法。

【請求項4】ネットワーク端末をノードチャラル間接通信ドメイン(VBDS:

140)に接続するための構造体であつて、
ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネット

トワーク端末から愛憎する手段と、
ユーチャを識別する情報から以上とのVBDを含むユーチャの属する接続グループを決定する手段と、
前記ネットトワーク端末が接続される以上のVBDを決定する手段であつて、前記
1段以上のVBDが前記接続グループのメンバであるような前記決定手段と、
前記ネットトワーク端末を前記1以上のVBDに接続するためのコマンドを発行する
手段とを含むことを特徴とする構造体。

【請求項5】 各VBDが、前記トライックが生じる前記VBDへの前記通信
トライックを制限可能なドメイン（116P）のサブドメインであり、
前記接続グループが、少なくとも2つのドメインからVBDを含み、
前記ネットトワーク端末が接続された以上でのVBDが、前記ネットトワーク端末を含
む前記ドメインに基づき決定されることを特徴とする請求項4に記載の構造体。

【請求項6】 各VBDがVLANであり、また前記ネットトワーク端末が、前記
接続グループに属するVLAN並びに前記ネットトワーク端末を含む前記ドメインに接
続されることを特徴とする請求項5に記載の構造体。

【請求項7】 前記構造体が、（1）所定のコンピュータシステム（12
4M）、及び（2）前記コンピュータシステムにロードされた所定のプログラム
を含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々
を含むことを特徴とする請求項4に記載の構造体。

【請求項8】 前記構造体が、所定のコンピュータの読み取り可能な媒体で
あり、そこで各手段が、1以上のコンピュータの命令、コンピュータの読み取り可
能なデータ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求
項4に記載の構造体。

【請求項9】 ネットトワークドメイン（116P、116Q、116R、
116S、116T）間のトライックの経路を指定する以上の装置（130
）に対して1以上のアクセス制御リスト（ACLs）を生成するための方法において
、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記
ドメイン間ににおいてどのようなトライックが許可及び／又は拒否されるかを決
定し、更に、

サブネットワークの各グループ内においてトラフィックが許可されるようになり、各サブネットワーク（1.4.0.a、1.1.6.T）の1以上の中のグループを規定する過程であつて、各サブネットワークがネットワークの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、

前記コンピュータシステムが、各グループ内のトラフィックを許可するためには1以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項1.01】 前記1D以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを拒否する前記複数のグループを規定する過程を含むことを特徴とする請求項9に記載の方法。

【請求項1.1】 1D以上の共用サブネットワークの識別子を受譲する前記コンピュータシステムを用いた前記方法において、トラフィックが、前記グループの何れか一つにおける各共用ネットワークと任意の別のサブネットワークの間において許可され、

1D以上のACLによって、トラフィックが、前記グループの何れか一つにおける前記共用サブネットワークの何れか一つと任意のサブネットワークとの間ににおいて許可されることを特徴とする請求項9に記載の方法。

【請求項1.2】 少なくとも1つの前記ドメインか、前記ドメインにおいてトラフィックを制限することが可能であるような前記方法であつて、1D以上のグループの各々に対して、前記コンピュータシステムが、前記グループ内において許可及び／又は拒否されたトラフィックを識別するための情報を受信する過程であつて、前記情報を、制限するトラフィックにおける1Dのメインによって使用されるような前記受信過程と、

前記情報による指定に従つてトラフィックを制限可能な各ドメインを構成する過程とを含むことを特徴とする請求項9に記載の方法。

【請求項1.3】 所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1以上上の（1）トラフィックを制限可能な

ドメイン内のトラフィックを各々送信するID以上のスイッチ（1128）のポート（1160）であつて、前記グループ内のトラフィックを運ぶための前記ポート（1160）と、（2）前記グループに属するエンティティ（1124）の物理的アドレスと、更に（3）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項12に記載の方法。

【請求項14】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項9に記載の方法。

【請求項15】 前記11以上の表記が、IPアドレスに接つきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項9に記載の方法。

【請求項16】 ネットワークドメイン（116P、116Q、116R、116S、116T）間のトラフィックの経路を指定する以上の装置（1130）に対して以上のアクセス制御リスト（ACLs）を生成するための所定の構造体において、そのような構造にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間においてどのようなトラフィックが許可度で／又は拒否されるかを決定し、更に、各グループ内においてトラフィックが許可されるよう、サブネットワーク（1140、116）のID以上のグループをコンピュータシステムに対しても定する手段であつて、各サブネットワークがネットワークメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって讀取るための前記規定手段と、

前記コンピュータシステムによって、各グループ内のトラフィックを許可するためのACLを生成するための手段とを含むことを特徴とする構造体。

【請求項17】 前記構造体が、前記コンピュータシステム（1124M）及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項16に記載の構造体。

【請求項18】 前記構造体が、前記規定手段及び前記生成手段を実施す

るための命令を含むコンピュータの読み取り可能な媒体であることを特徴とする請求項 1.6 に記載の構造体。

【請求項 1.9.1】 前記規定手段が複数のグループを規定するときに、前記 1.8 上のACLが異なるグループ内におけるサブネットワーク間のトラフィックを拒否することを特徴とする請求項 1.6 に記載の構造体。

【請求項 2.0】 1.以上との共用サブネットワーク（1.16.S）の識別子を前記コンピュータシステムによって読み取るための手段を更に含む前記構造体において、前記グループとの間でトラフィックが許可され、1.以上の前記ACLによって、前記グループの何れか一つにおける前記共用サブネットワークの何れか一つと併用のサブネットワークとの間でトラフィックが許可されることを特徴とする請求項 1.6 に記載の構造体。

【請求項 2.1】 少なくとも 1 つの前記ドメインが、前記ドメインにおいてトラフィックを制限可能であるような前記構造体であって、1.以上のグループの各々に対して、前記グループ内における許可及び／又は拒否されたトラフィックを識別するための情報を前記ユニバータシスティムによつて読み取るための手段であつて、前記情報が、トラフィックの制限において1.以上のドメインによって使用されるような読み取り手段と、

前記情報による指定に従つてトラフィックを許可及び／又は拒否するように、トラフィックを制限可能な各ドメインを前記ユニバータシスティムによって構成するための手段とを更に含むことを特徴とする請求項 1.6 に記載の構造体。

【請求項 2.2】 所定のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1.以上の（1）トラフィックを制限可能なドメイン内のトラフィックを各々送信する以上のスイッチ（1.2.8）のポート（1.6.0）であつて、前記グループ内のトラフィックを運ぶための前記以上のポート（1.6.0）と、（2）前記グループ内に属するエンティティの物理的アドレスと、更に（3）前記グループ内に属するトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項 2.1 に記載の構造体。

【請求項 2.3】 各サブネットワークの識別子が、アドレス又はアドレス

レンシであることを特徴とする請求項 1 6 に記載の構造体。

【請求項 2 4】 前記 1 以上の装置が、IP アドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的なアドレスに基づき端末間で送信されることを特徴とする請求項 1 6 に記載の構造体。

【請求項 2 5】 復数のドメイン (1 1 6) を含む所定のネットワークにおける接続を確立するための方法において、各ネットワーク端末が、第 1 の型のアドレス及び第 2 の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトラフィックが、祖先ネットワーク端末の第 2 の型のアドレスを用いることなしに、前記祖先ネットワーク端末の第 1 の型のアドレスを使用して前記祖先ネットワーク端末に送信され、一方でドメイン間においては、前記祖先ネットワーク端末の第 2 の型のアドレスを使用してトラフィックが送信され、また制限され、ドメインが同一のサブドメイン内のトラフィックを許可し、一方でサブドメインのトラフィックを拒否するように、少なくとも 1 つのドメインが、前記ドメインにおいて規定されたサブドメイン (1 4 0) を有することが可能であり、更に、

接続グループ C G 1 に属するトラフィックを規定する情報 I N F 1 をコンピュータシステム (1 2 4 M) に与える過程であって、前記接続グループ C G 1 が、種々のドメインにおいてサブドメインを有するためのものであり、それらの少なくとも 2 つがサブドメインへのトラフィックをそれぞれ制限可能であるような前記過程と、

少なくとも前記接続グループ C G 1 について、ドメインが、前記第 2 の型のアドレスを用いることなしに前記第 1 の型のアドレスを使用してトラフィックを送信するときに、前記ドメイン D 1 が前記情報 I N F 1 によって規定されたトラフィックを許可し、一方でサブドメイン S D 1 へのそのようなトラフィックを制限するよう、前記コンピュータシステムが、前記接続グループ C G 1 におけるサブドメイン S D 1 を有する各ドメイン D 1 を生成する過程とを含むことを特徴とする方法。

【請求項26】 トライフィックを規定する前記情報が、少なくとも1つのグループに対して、1以上の(1)車ーのドメイン内のトライフィックを各々送信する以上のスイッチ(128)のポート(160)であつて、前記グループ内のトライフィックを運ぶための以上の前記ポート(160)と、(2)前記グループ内のメンバである端末(124)の物理的アドレスと、更に、(3)前記グループ内のトライフィックの送信又は受信を許可されたユーザ名との識別子を含むこと特徴とする請求項25に記載の方法。

【請求項27】 各々のドメインを構成する過程が、前記グループにおけるサブドメインを有する車ーのドメイン内のトライフィックを送信するスイッチについて、(a)前記グループのメンバである端末の物理的アドレス間のトライフィックを許可するための、また(b)異なるグループのメンバである端末の物理的アドレス間のトライフィックを構成するための前記スイッチを構成すること特徴とする請求項26に記載の方法。

【請求項28】 複数のドメイン(116)を含む所定のネットワークにおいて、各ネットワーク端末が、第1の型のアドレス及び第2の型のアドレスを有することが可能であり、各ドメインにおけるネットワーク端末間のトライフィックが、宛先ネットワーク端末の第2の型のアドレスを用いることなしに、前記宛先ネットワーク端末の第1の型のアドレスを使用して前記宛先ネットワーク端末に送信され、一方でドメイン間ににおいては、前記宛先ネットワーク端末の第2の型のアドレスを使用してトライフィックが送信され、また制限され、

ドメインが車ーのサブドメイン内のトライフィックを許可し、一方でサブドメイン間のトライフィックを拒否するよう、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメイン(140)を有することが可能であり、更に、接続グループCC1に属するトライフィックを規定する情報INP1をコンピューターシステム(124M)によって送信するための手段であつて、前記接続グループCC1が、種々のドメインにおいてサブドメインを有するためのものであり

、それらの少なくとも2つがサブドメインへのトラフィックをそれぞれ制限可能であるような前記受信手段と、少なくとも1つの接続グループについて、前記接続グループのメンバであるサブドメインの識別子を前記コニビュータシステムによって愛信する手段と、少なくとも前記接続グループC.G.1について、ドメインが、前記第2の型のアドレスを用いることなしに前記第1の型のアドレスを使用してトラフィックを送信する手段と、前記ドメインD.1が前記情報LINE1によって規定されたトラフィックを許可し、一方でサブドメインSD.1へのそのようなトラフィックを制限するよう、前記接続グループC.G.1におけるサブドメインSD.1を有する各ドメインD.1を前記コニビュータシステムによって構成するための手段とを有することを特徴とする構造体。

【請求項29】 トライックを規定する前記情報が、少なくとも1つのグループに対して、以下の(1)車……のドメイン内のトライックを各々送信する以上のスイッチ(128)のポート(160)であって、前記グループ内のトライックを運ぶための以下の前記ポート(160)と、(2)前記グループのメンバである端末(124)の物理的アドレスと、更に(3)前記グループ内のトライックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項28に記載の構造体。

【請求項30】 前記構造体が、前記コンピュータシステム及び終コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項28に記載の構造体。

【請求項31】 前記全ての手段を実施するための命令を含むコンピュータの読み取り可能媒体であることを特徴とする請求項28に記載の構造体。

【請求項32】 各ドメイン内のトライックが、端末の物理的アドレスに基づき端末間で送信され、またドメイン間のトライックが、端末の論理的アドレスに基づき経路指定されることを特徴とする請求項28に記載の構造体。

【手続補正2】

【補正対象箇類名】明細書

【補正対象項目名】 0003

【補正方法】 義更

【補正内容】

【0003】

これについて図1及び図2に示す(これらの場合には先行技術にはない、本発明の幾つかの態様が示してある)。ネットワーク110は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク110には、『第2層ドメイン(1ayer 2 domains)』116P、116R、116Q、116S、116Tが含まれる(用語『第2層』は、D. Biererらの"Netware4 for Professionals" (1993), 1-9頁に記載のOSI参照モデルのを指す)。同様の第2層ドメイン116に属する端末124(例えば、ドメイン116Pにおける端末124, 1, 124, 2)は、それらのMACアドレス(第2層アドレス)を用いて互いに通信可能である。MAC(媒体アクセス制御)アドレスは、端末のネットワークインターフェースカード(NIC)に書き込まれた物理的アドレスであるか、又はNICスイッチの設定によって確立された物理的アドレスである。全てのドメイン116又はその幾つかには、IEEE上のネットワークスイッチ(NICスイッチ)と連携しない)が含まれる。各ドメイン116のスイッチ128は、端末のMACアドレスを用いて端末124間でトライックを送信する。

【手続補正3】

【補正対象図類名】 明細書

【補正対象項目名】 0023

【補正方法】 義更

【補正内容】

【0023】

ユーザ名によるVLANのメンバーシップの確定について、付録Aに記載されている。("User-Based Binding of Network Stations to Broadcast Domains"と題するJ. Ekstromらの米国特許第5,968,126号(1999年10月19日発行)を参照)。これについては、ここで言及することにより本明細書の一部とする。)或る実施例においては、VLAN140が、ポートによって識別される端末、MACアドレスに

よつて識別される端末、及び／又は……が名によつて識別される端末を結合づけける。

INTERNATIONAL SEARCH REPORT

Classification: Confidential - Search Report
Case ref: PCT/US99/08866

International Search Report	
Classification: Confidential - Search Report	PCT/US99/08866
Case ref: PCT/US99/08866	International Search Report
A	<p>SAUNDERS, S.: "SWITCH PLTS VIRTUAL LANS ON AUTOMATIC PILOT. AGILE'S VIRTUAL SWITCH IS THE FIRST TO AUTOMATE SETUP OF VIRTUAL WORKGROUPS COMMUNICATIONS, VOL 2, NUMBER 12, 1993 (1994-09-01). PAGES 45-46, XPO06422380, ISSN 1063-6399, THE WHOLE DOCUMENT." 1, 4, 9, 13, 16, 25, 28</p> <p>YXNEKES, G. H.: "DIFFERING APPROACHES TO VIRTUAL LANs" BUSINESS COMMUNICATIONS REVIEW, DECEMBER 1993 (1993-12), PAGES 42-45, XPO0661940, ABSTRACT</p>

(54)

特許2002-513245

INTERNATIONAL SEARCH REPORT

Information on patentability presented

Examination documents used in search report		Publication date	Patent family	Publication date
WD	9302821	A 22-01-1998	A3 3128497 A 2310285 A	09-02-1998 15-04-1999
EP	0312056	A 10-12-1997	JP 10056473 A	26-03-1998

Patent Application No.
PCT/JP 96/08366

Entered into International Registration	Entered into National Registration

プロントベーションの統合

(6) 組定期
E P (A T), B E, C H, C Y,
D E, D K, E S, F T, F R, G B, G R, I E, I
T, L U, M C, N L, P T, S E), O A (B F, B J
, C F, C G, C I, C M, G A, G N, G W, M L,
M R, N E, S N, T D, T G), A P (G H, G M, K
E, L S, M W, S D, S L, S Z, U G, Z W, E
A (A M, A Z, B Y, K G, K Z, M D, R U, T J
, T M), A E, A L, A M, A T, A U, A Z, B A
, B B, B C, B R, B Y, C A, C H, C N, C U,
C Z, D E, D K, E E, E S, F I, G B, G D, G
E, G H, G M, H R, H U, I D, I G, I N, I S
, J P, K E, K G, K P, K R, K Z, L C, L K,
L R, L S, L T, L U, L V, M D, M G, M K, M
N, M W, M X, N O, N Z, P L, P T, P Q, R U
, S D, S E, S C, S I, S K, S L, T J, T M,
T R, T T, U A, U G, U Z, V N, Y U, Z A, Z
W

(7) 組別語 エクストロム、ジョセフ・エクセイ

アメリカ合衆国エクタ州84042・9-ドレジ

イースト 300サウス、131

モス、スティーブンズ

アメリカ合衆国ミシシッピ州84042・リバード

ノース 450アーヴィントン 298

【統合の統合】
によつて制限される。